Counting Cubic Number Fields

Niven Achenjang

December 2020

Contents

1 Cubic Rings and Binary Cubic Forms **3**

1.1 The Correspondence . . . 3

1.2 Local Densities of Maximal Rings . . . 7

2 Counting Cubic Rings **9**

2.1 The Setup . . . 10

2.2 The Count . . . 14

2.2.1 Averaging Trick . . . 14

2.2.2 Estimating Lattice Points . . . 16

2.3 Including Congruence Conditions . . . 19

3 Wrapping Things Up **20**

3.1 Counting Cubic Number Fields . . . 20

3.2 Average Size of 3-torsion in Class Groups of Quadratic Number Fields . . . 22

Introduction

We aim to give an account of the theorems of Davenport and Heilbronn [DH71] giving an asymptotic count for the number of cubic number fields of bounded (positive or negative) discriminant. In particular, our main theorem will be the following.

Theorem 1 ([DH71], Theorem 1)**.** *Let $N_3(\xi, \eta)$ denote the number of cubic number fields K, up to isomorphism, satisfying $\xi < \operatorname{Disc}(K) < \eta$. Then,*

$$\begin{aligned} N_3(0, X) &= \frac{1}{12\zeta(3)}X + o(X); \\ N_3(-X, 0) &= \frac{1}{4\zeta(3)}X + o(X). \end{aligned}$$

While this result is originally due to Davenport-Heilbronn, our account of it will most closely follow that of Bhargava, Shankar, and Tsimerman in [BST13].[1] For us, our main motivation for considering the above theorem comes from arithmetic statistics.

[1] 'closely follow' in a strong sense. I think in the end these notes ended up being essentially a rewrite of the relevant sections of their paper with some added details at points I found more confusing.

There is interest in understanding how the class group Cl_K of a number field K changes, as one varies the field K. Restricting attention to quadratic number fields, one way of turning this curiosity into a precise question is to first consider the uniform distribution μ_X^+ ($X > 0$) on isomorphism classes of quadratic number fields K with positive discriminants $0 < \operatorname{Disc} K < X$. Roughly speaking, μ_X^+ pushes forward, via Cl_K, to a distribution $\mathrm{Cl}_{\mu_X^+}$ on finite, abelian groups which captures information about the statistical behavior of class groups of real quadratic numbers of bounded discriminant; one can then take limits as $X \to \infty$ to probe the behavior of class groups of all real quadratic number fields. Cohen and Lenstra [CL84] made precise predictions about the limiting distribution $\nu^+ := \lim_{X\to\infty} \mu_X^+$ obtained in this way, as well as about the analogous distribution ν^- which captures information about class groups of imaginary quadratic number fields. In particular, their predictions would imply that

$$\begin{aligned}\lim_{X\to\infty} \mathbb{E}_{K\sim\mu_X^+}\left[\#\operatorname{Sur}\left(\mathrm{Cl}_K, \frac{\mathbb{Z}}{3\mathbb{Z}}\right)\right] &= \left|\frac{\mathbb{Z}}{3\mathbb{Z}}\right|^{-1} = \frac{1}{3}\\ \lim_{X\to\infty} \mathbb{E}_{K\sim\mu_X^-}\left[\#\operatorname{Sur}\left(\mathrm{Cl}_K, \frac{\mathbb{Z}}{3\mathbb{Z}}\right)\right] &\qquad\qquad = 1\end{aligned}$$

The relevance of this brief discussion of class group statistics to our stated task of counting cubic number fields is that we will see that, as a by-product of our main result, we will also obtain asymptotics for the average size of $\#\,\mathrm{Cl}_K[3]$, the size of the 3-torsion of the class groups of *quadratic* number fields K. Since Cl_K is a finite abelian group, one has

$$\#\operatorname{Sur}(\mathrm{Cl}_K, \mathbb{Z}/3\mathbb{Z}) = \#\operatorname{Hom}(\mathrm{Cl}_K, \mathbb{Z}/3\mathbb{Z}) - 1 = \#\operatorname{Hom}(\mathbb{Z}/3\mathbb{Z}, \mathrm{Cl}_K) - 1 = \mathrm{Cl}_K[3] - 1,$$

so understanding $\#\,\mathrm{Cl}_K[3]$ is enough to verify one part of Cohen and Lenstra's predictions. With that said, Davenport and Heilbronn calculated the average size of 3-torsion in the class groups of quadaratic number fields.

Theorem 2 ([DH71], Theorem 3)**.** *Let D denote the discriminant of a quadratic field and let $\mathrm{Cl}_{\mathbb{Q}(\sqrt{D})}[3]$ denote the 3-torsion subgroup of the ideal class group $\mathrm{Cl}_{\mathbb{Q}(\sqrt{D})}$ of $\mathbb{Q}(\sqrt{D})$. Then,*

$$\begin{aligned}\sum_{0<D<X} \#\,\mathrm{Cl}_{\mathbb{Q}(\sqrt{D})}[3] &= \frac{4}{3}\cdot \sum_{0<D<X} 1 + o(X);\\ \sum_{-X<D<0} \#\,\mathrm{Cl}_{\mathbb{Q}(\sqrt{D})}[3] &= 2\cdot \sum_{-X<D<0} 1 + o(X).\end{aligned}$$

That is, $\mathbb{E}_{K\sim\mu_X^+}[\#\,\mathrm{Cl}_K[3]] = \frac{4}{3} + o(1)$ and $\mathbb{E}_{K\sim\mu_X^-}[\#\,\mathrm{Cl}_K[3]] = 2 + o(1)$.

The proof of Theorem 1 will proceed in several steps. The main idea is that every cubic number field K has a unique cubic ring $\mathscr{O}_K$, its ring of integers, attached to it; to count cubic number fields, we count cubic rings and then pick from this count those cubic rings which appear as the ring of integers of some number field. In order to count cubic rings, we will make use of a nice correspondence between then and binary cubic forms $f(x,y) = ax^3 + bx^2y + cxy^2 + dy^3$, which are more readily amenable to counting. We will begin by setting up this correspondence. The brunt of the argument is then spent on using it to count binary cubic rings. Finally, we use a sieve to extract counts of maximal cubic rings (equivalently, of cubic number fields), proving Theorem 1. A similar sieve along with some class field theory is then used to obtain Theorem 2.

1 Cubic Rings and Binary Cubic Forms

1.1 The Correspondence

We wish to set up a correspondence between cubic rings and binary cubic forms. In fact it will be useful to have such a correspondence not only for rings, but for algebras, e.g. over $\mathbb{Z}_p$ or $\mathbb{F}_p$, as well. Hence we work in a slightly general setting.

Fix a domain A. For our applications we will mostly take $A = \mathbb{Z}, \mathbb{Z}_p, \mathbb{F}_p$.

Definition 1.1. A **cubic A-algebra** is a commutative A-algebra R which is free of rank 3 as an A-module.

These will be in bijection with $\mathrm{GL}_2(A)$-orbits of binary cubic forms $f(x,y) = ax^3 + bx^2y + cxy^2 + dy^3$ $(a,b,c,d \in A)$under the action

$$(\gamma \cdot f)(x,y) := \frac{1}{\det \gamma} f\left((x,y)\cdot\gamma\right),$$

where $\gamma \in \mathrm{GL}_2(A)$. Indeed,

Theorem 1.2 ([GGS02], Proposition 4.2)**.** *There is a natural bijection between the set of* $\mathrm{GL}_2(A)$*-equivalence classes of binary cubic A-forms, and the set of isomorphism classes of cubic rings.*

Proof. Given a cubic A-algebra R, let $\langle 1, \omega, \theta\rangle$ be an A-basis, and temporarily write $\omega\theta = u + v\omega + w\theta$ with $u, v, w \in A$. Then,

$$(\omega - w)(\theta - v) = (u + v\omega + w\theta) - v\omega - w\theta + vu = u + vw \in A,$$

so we can replacing ω, θ with $\omega - w, \theta - v$, respectively, to assuming that we have a **normal basis**, i.e. one where $\omega\theta \in A$.

Since $\langle 1, \omega, \theta\rangle$ is a normal basis, there exists constants $a, b, c, d, \ell, m, n \in A$ such that

$$\begin{aligned} \omega\theta &= n \\ \omega^2 &= m - b\omega + a\theta \\ \theta^2 &= \ell - d\omega + c\theta. \end{aligned} \tag{1.1}$$

To R, we associate the binary cubic form $f(x,y) = ax^3 + bx^2y + cxy^2 + dy^3$.

Conversely, given a binary cubic form $f(x,y) = ax^3 + bx^2y + cxy^2 + dy^3$, referring to (1.1) almost immediately gives us the multiplication law on our desired cubic algebra. We require $(\omega\theta)\theta = \omega(\theta^2)$, which tells us that $n = -ad$ and $\ell = -bd$, as well as$(\omega^2)\theta = \omega(\omega\theta)$, which tells us that $m = -ac$. Making the assignments

$$\begin{aligned} n &= -ad \\ m &= -ac \\ \ell &= -bd \end{aligned} \tag{1.2}$$

in (1.1) gives us our cubic A-algebra $R = R_A(f)$, along with a preferred normal basis for it.

This sets up correspondence between cubic rings with normal bases and binary cubic A-forms. To see that changing the normal basis exactly corresponds to acting on the associated form by some element of $\mathrm{GL}_2(\mathbb{Z})$, we introduce a coordinate-free perspective for our bijection. The form $f(x, y)$ represents the cubic map $A^2 \cong R/A \to \bigwedge^2(R/A) \cong A$ given by $r \mapsto r \wedge r^2$. For $r = x\omega + y\theta$, one has

$$r \wedge r^2 = f(x, y)(\omega \wedge \theta).$$

In particular, changing the A-basis (ω, θ) for R/A by an element $\gamma \in \mathrm{GL}_2(A)$, and then renormalizing this basis in R transforms the corresponding binary cubic form $f(x, y)$ by that same element of $\mathrm{GL}_2(A)$. ■

Notation 1.3. When $A = \mathbb{Z}$, we will usually write $R(f)$ in place of $R_{\mathbb{Z}}(f)$.

Remark 1.4. Combining (1.2) and (1.1), passing back and forth between a cubic A-algebra and its associated binary cubic is achieved by using the following equations.

$$\begin{aligned} \omega\theta &= -ad \\ \omega^2 &= -ac - b\omega + a\theta \\ \theta^2 &= -bd - d\omega + c\theta. \end{aligned} \tag{1.3}$$

This sets up our correspondence. We would not like to be able to read off properties of the ring $R_A(f)$ by just looking at the form f itself.

Definition 1.5. Let R be a cubic A-algebra. The **trace** of an element $\alpha \in R$, denoted $\mathrm{Tr}_A\,\alpha$, is the trace of the A-linear operator $m_\alpha : R \to R$ given by multiplication by α. This allows us the define a bilinear pairing $(\alpha, \beta) \mapsto \mathrm{Tr}_A(\alpha\beta)$ on R. The determinant of this pairing is called the **discriminant** of R, and is denote $\mathrm{Disc}_A\,R$.

Definition 1.6. Let $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$ be a binary cubic. Its **discriminant** is degree 4 homogeneous polynomial

$$\mathrm{Disc}(f) := b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd.$$

One can check that, for $g \in \mathrm{GL}_2(\mathbb{R})$, $\mathrm{Disc}(g \cdot f) = (\det g)^4\,\mathrm{Disc}(f)$.

Proposition 1.7. *The discriminant of a binary cubic is equal to the discriminant of its corresponding algebra.*

Proof Sketch. One can just go through the trouble of computing this by hand. ■

The above proposition is useful since we will be counting by discriminant. Recall that we will later want to pick out the cubic rings which correspond to rings of integers of number fields. The first step in doing this will be telling when $R_A(f)$ is a domain.

Proposition 1.8. *For an integral binary cubic A-form f, the cubic A-algebra $R(f)$ is an integral domain iff f is irreducible as a polynomial over $F := \mathrm{Frac}\,A$.*

Proof. If f is reducible, it must have a linear factor[2] which, by change of variable in $\mathrm{GL}_2(A)$, we may assuming is y, i.e. we may assume $a = 0$. Hence, by (1.3), $\omega\theta = -ad = 0$ too, so $R(f)$ is not a domain.

Conversely, suppose R has zero divisors. We first claim that there exists $\omega \in \mathbb{R}$ such that $\langle 1, \omega\rangle \subset R$ is a quadratic subalgebra. We construct it as follows. Let α and β be two nonzero elements of R with $\alpha\beta = 0$, and let $\alpha^3 + c_1\alpha^2 + c_2\alpha + c_3 = 0$ be the characteristic equation of the A-linear mapping $\alpha : R \to R$. Multiplying both sides by β, we see that $c_3 = 0$, so $\alpha(\alpha^2 + c_1\alpha + c_2) = 0$. Recall that we're not working in a domain. If $\alpha^2 + c_1\alpha + c_2 = 0$, then we can set $\omega = \alpha$ (so $\omega^2 = -c_1\omega - c_2$). Otherwise,

$$(\alpha^2 + c_1\alpha + c_2)^2 = \alpha^2(\alpha^2 + c_1\alpha + c_2) + c_1\alpha(\alpha^2 + c_1\alpha + c_2) + c_2(\alpha^2 + c_1\alpha + c_2) = c_2(\alpha^2 + c_1\alpha + c_2),$$

in which case we can take $\omega = (\alpha^2 + c_1\alpha + c_2)$ (and $\omega^2 = c_2\omega$).

Scaling ω by an integer if necessary, we may assume that it is a primitive vector in the lattice $R \cong \mathbb{Z}^3$, and then extend $\langle 1, \omega\rangle$ to a basis $\langle 1, \omega, \theta\rangle$ of R. Normalizing this basis if needed, we have $\omega^2 \in \langle 1, \omega\rangle$ so $a = 0$ by comparison with (1.3). Hence, the associated binary cubic form is reducible. ■

To take this a step further, we temporarily set $A = \mathbb{Z}$. A cubic ring $R = R_{\mathbb{Z}}(f)$ will be the ring of integers of some field if it is a domain and furthermore is a maximal order in its fraction field. Note that R is maximal iff $R_p := R \otimes \mathbb{Z}_p = R_{\mathbb{Z}_p}(f)$ is maximal for all p. Hence, maximality is best checked locally, and the following result characterizes the ways in which local maximality can fail. If R_p is maximal, we say that R is "**maximal at** p."

Lemma 1.9. *Suppose R is a cubic ring (i.e. $\mathbb{Z}$-algebra) which is not maximal at p. Then, there is a $\mathbb{Z}$-basis $\langle 1, \omega, \theta\rangle$ of R such that at least one of the following is true*

- $\mathbb{Z} + \mathbb{Z} \cdot (\omega/p) + \mathbb{Z} \cdot \theta$ *forms a ring*
- $\mathbb{Z} + \mathbb{Z} \cdot (\omega/p) + \mathbb{Z} \cdot (\theta/p)$ *forms a ring*

Proof. Let $R' \supset R$ be a ring strictly contining R such that the index of R in R' is a multiple of p, and let $R_1 = R' \cap (R \otimes_{\mathbb{Z}} \mathbb{Z}[1/p])$. Then, R_1 also strictly contains R, and the index of R in R_1 is a power of p. Since $R \subset R_1$ is a p-power inclusion of f.g. free $\mathbb{Z}$-modules, the structure theorem for modules over a PID guarantees the existence of nonnegative integers $i \geq j$ along with a basis $\langle 1, \omega, \theta\rangle$ of R such that

$$R_1 = \mathbb{Z} + \mathbb{Z}(\omega/p^i) + \mathbb{Z}(\theta/p^j).$$

If $i = 1$ (so $j \in \{0, 1\}$) we win, so assume $i > 1$. We normalize the basis $\langle 1, \omega, \theta\rangle$ if necessary. Recalling (1.3), that the RHS above is a ring translates into the following conditions:

$$\begin{aligned} a &\equiv 0 \pmod{p^{2i-j}} \\ b &\equiv 0 \pmod{p^i} \\ c &\equiv 0 \pmod{p^j} \\ d &\equiv 0 \pmod{p^{2j-i}}. \end{aligned}$$

[2] e.g. because $f(x, y)$ splits into 3 (homogeneous) linear factors over $\overline{F}$ since it is homogeneous in two variables.

If $j = 0$, then we can replace (i, j) by $(i-1, j)$ while maintaining the truth of the above congruences. If $j > 0$, then replacing (i, j) by $(i-1, j-1)$ maintains the above congruences. Thus, in a finite sequence of moves, we arrive at $i = 1$ as desired. ■

This lemma gives two ways a cubic ring $R(f)$ could fail to be maximal at p: **(i)** f is a multiple of p or **(ii)** there is a $\mathrm{GL}_2(\mathbb{Z})$-translate of $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$ where $p^2 \mid a$ and $p \mid b$. Thus, it shows

Corollary 1.10. *Let $\mathcal{U}_p$ be the set of binary cubic forms f not satisfying either of the two conditions. The cubic ring $R(f)$ is maximal at p iff $f \in \mathcal{U}_p$. It is maximal iff $f \in \mathcal{U}_p$ for all p.*

There are two more facts about this correspondence which will come handy in later arguments. First, sticking with the case $A = \mathbb{Z}$, f allows us to see the number of index p subrings of R. This will show up when we perform our sieves at the end.

Proposition 1.11. *For an integral binary cubic form f, the number of index p subrings of $R(f)$ is equal to $\omega_p(f)$, the number of zeros in $\mathbb{P}^1(\mathbb{F}_p)$ of f modulo p.*

Proof. First, if $R' \subset R$ with index p, then $R' = \mathbb{Z} + pR + \mathbb{Z}\theta$ for some well-defined element $\theta \in (R/\mathbb{Z})/p(R/\mathbb{Z})$. Extending this element to a $\mathbb{Z}$-basis $1, \omega, \theta$ of R', and renormalizing if necessary, we see that $1, \omega, \theta$ is a $\mathbb{Z}$-basis for R such that $1, p\omega, \theta$ is a $\mathbb{Z}$-basis for R. Note that θ is well-defined in $(R/\mathbb{Z})/p(R/\mathbb{Z})$ while $p\omega$ is well-defined in $(R'/\mathbb{Z})/p(R'/\mathbb{Z})$.

If $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$ is the binary cubic form corresponding to the normal basis $1, \omega, \theta \in R$, then (1.3) shows us that $R' = \mathbb{Z} + pR + \mathbb{Z}\theta$ is also a ring iff $\theta^2 \in R'$ iff $d \equiv 0 \pmod{p}$. Recall that we can view f as the cubic map $R/\mathbb{Z} \to \bigwedge^2(R/\mathbb{Z})$ given by $r \mapsto r \wedge r^2$. In particular, the image of $\theta \in R/\mathbb{Z}$ under this map is

$$\theta \wedge \theta^2 = -d\theta \wedge \omega \in \bigwedge^2(R'/\mathbb{Z}),$$

so R' is a ring iff θ is a root of $f \pmod{p}$. This gives the desired bijection between roots of $f \pmod{p}$ and subrings $R' \subset R$ of index p: from R' we can extract $\theta \in (R/\mathbb{Z})/p(R/\mathbb{Z})$ giving a root of $\overline{f} : (R/\mathbb{Z})/p(R/\mathbb{Z}) \to \bigwedge^2[(R/\mathbb{Z})/p(R/\mathbb{Z})]$; from a root $\overline{\theta}$ of f mod p, we can lift this to some $\theta \in R$ and then form $R' = \mathbb{Z} + pR + \mathbb{Z}\theta$ which will be a genuine subring by the preceding iff's. ■

The final fact about this correspondence we will need is that automorphisms of cubic algebras correspond to stabilizers of the GL_2-action. In particular, we return to A being an arbitrary domain.

Proposition 1.12. *For a binary cubic A-form f, the group of A-algebra automorphisms of $R(f)$ is naturally isomorphic to the stabilizer of f in $\mathrm{GL}_2(A)$.*

Proof. Any A-algebra automorphism φ of $R(f)$ gives a $\mathrm{GL}_2(A)$-transformation on the chosen normal basis ω, θ of R/A – and the transformed basis has the same multiplication table – so gives an element of the stabilizer of the binary cubic form f in $\mathrm{GL}_2(A)$. Conversely, if

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathrm{GL}_2(A)$$

stabilizes f, then

$$\varphi : \begin{pmatrix}1\\ \omega\\ \theta\end{pmatrix} \mapsto \begin{pmatrix}1\\ p\omega + r\theta\\ q\omega + s\theta\end{pmatrix}$$

extends to an A-algebra automorphism of $R(f)$ since it preserves the multiplication table. ■

This wraps up out discussion of the correspondence between cubic rings and binary cubic forms. The most important points are that it preserves discriminants and allows us to test for maximality, but of course, the other properties shown here will be needed as well.

1.2 Local Densities of Maximal Rings

Recall that our rough strategy is to count cubic rings, and then pick out the ones which are maximal. Doing so will essentially involving answering the questions, "What proportion of cubic rings are maximal?" Since our understanding of maximality is local, a perhaps better question to answer at the onset is, "what proportional of cubic rings are maximal at p?" If one imagines that maximality at various primes are independent conditions, then the proportion of cubic rings which are maximal (everywhere) should be expressible as a product of the analogous proportions of each prime. We will make this rigorous when performing the sieve at the end; for now, we tackle the local proportionality question.

Notation 1.13. Given a domain A, let V_A denote the rank r free A-module of binary cubic forms over A. We will primarily be interested in $A = \mathbb{Z}, \mathbb{Z}_p, \mathbb{F}_p$.

Let A be one of $\mathbb{Z}, \mathbb{Z}_p, \mathbb{F}_p$, and consider some binary cubic form f over A such that $f \not\equiv 0 \pmod{p}$. Then, one can write

$$R_A(f)/(p) \cong \mathbb{F}_{p^{f_1}}[t_1]/(t_1^{e_1}) \oplus \cdots \oplus \mathbb{F}_{p^{f_g}}[t_g]/(t_g^{e_g}).$$

Since $R_A(f)$ is a cubic A-algebra, comparing $\mathbb{F}_p$-dimensions of both sides shows that

$$3 = \sum_{i=1}^{g} f_i e_i.$$

We record this information by defining the symbol $(f,p) := \left(f_1^{e_1} f_2^{e_2} \dots f_g^{e_g}\right)$; its possible values are

$$(111),\ \ (12),\ \ (3),\ \ (1^2 1),\ \text{ and }\ (1^3).$$

Remark 1.14. The symbol (f,p) indicates the factorization of $f \pmod{p}$. Specifically $(f,p) = \left(f_1^{e_1} f_2^{e_2} \dots f_g^{e_g}\right)$ if and only if

$$f(x,y) \equiv h_1^{e_1}(x,y) \dots h_g^{e_g}(x,y) \pmod{p},$$

where $h_i(x,y)$ is irreducible over $A/(p)$, and $\deg h_i = f_i$. Equivalently, $(f,p) = \left(f_1^{e_1} f_2^{e_2} \dots f_g^{e_g}\right)$ if and only if $f \pmod{p}$ has g roots, the ith of which is defined over $\mathbb{F}_{p^{f_i}}$ and appears with multiplicity e_i.

Thinking in these terms allows us to easily the determine the density of each factorization type.

Notation 1.15. We let $T_p(f_1^{e_1} \dots f_g^{e_g}) \subset V_{\mathbb{Z}_p}$ denote the set of forms f such that $(f,p) = (f_1^{e_1} \dots f_g^{e_g})$.

Notation 1.16. For any $S \subset V_{\mathbb{Z}}$ (or $V_{\mathbb{Z}_p}$), we let $\mu_p(S)$ denote the p-adic density of the p-adic closure of S in $V_{\mathbb{Z}_p} \cong \mathbb{Z}_p^4$. The measure μ_p is normalized so that $\mu_p(\mathbb{Z}_p) = 1$.

Lemma 1.17. *We have*

$$\begin{aligned}
\mu_p(T_p(111)) =& \frac{1}{6}(p-1)^2 p(p-1)/p^4 \\
\mu_p(T_p(12)) =& \frac{1}{2}(p-1)^2 p(p+1)/p^4 \\
\mu_p(T_p(3)) =& \frac{1}{3}(p-1)^2 p(p+1)/p^4 \\
\mu_p(T_p(1^21)) =& \ \ (p-1)\ \ p(p+1)/p^4 \\
\mu_p(T_p(1^3)) =& \ \ (p-1)\ \ \ \ (p+1)/p^4
\end{aligned}$$

Proof Sketch. We only perform the calculation for $\mu_p(T_p(111))$. All the rest are done similarly. The main point is that membership in $T_p(\cdot)$ can be tested after passing to $f \pmod p$, so we might as well work over $\mathbb{F}_p$. Hence, $f \in T_p(111)$ iff it has 3 zeros in $\mathbb{P}^1$ defined over $\mathbb{F}_p$. The number of unordered triples of distinct points in $\mathbb{P}^1$ defined over $\mathbb{F}_p$ is precisely

$$\frac{1}{6}(\#\mathbb{P}^1)(\#\mathbb{P}^1 - 1)(\#\mathbb{P}^1 - 2) = \frac{1}{6}(p+1)p(p-1).$$

Given such a triple, there is, up to scaling, a unique binary cubic form having it as its set of roots. The total number of binary cubic forms over $\mathbb{F}_p$ is p^4, so this gives the claimed density

$$\mu_p(T_p(111)) = \frac{1}{6}(p+1)p(p-1)/p^4. \qquad \blacksquare$$

We now wish to use the above calculations to obtain the p-adic densities of the sets $\mathcal{U}_p$ consisting of forms maximal at p. Let $\mathcal{U}_p(\cdot) \subset T_p(\cdot)$ be the subset consisting of f such that $R(f)$ is maximal at p.

Remark 1.18. First consider $f \in T_p(111) \cup T_p(12) \cup T_p(3)$. Then, p is unramified in $R(f)$, so $p \nmid \operatorname{Disc}(f)$. However, if $R_{\mathbb{Z}_p}(f) \subset R'$ is contained in another cubic $\mathbb{Z}_p$-algebra, then it is an easy consequence of modules over a PID that

$$\operatorname{Disc}(R_{\mathbb{Z}_p}(f)) = [R' : R_{\mathbb{Z}_p}(f)] \operatorname{Disc}(R').$$

Since, $p \nmid \operatorname{Disc}(R_{\mathbb{Z}_p}(f))$, we conclude that $p \nmid [R' : R_{\mathbb{Z}_p}(f)]$, so $R_{\mathbb{Z}_p}(f) = R'$, showing that it is maximal.

Remark 1.19. Now consider $f \in T_p(1^21) \cup T_p(1^3)$. We can use a $\mathrm{GL}_2(\mathbb{Z})$-transformation to sen the unique multiple root of f in $\mathbb{P}^1_{\mathbb{F}_p}$ to the point $[1 : 0]$. Hence, we may assume

$$f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3 \text{ with } a \equiv b \equiv 0 \pmod p.$$

Recalling the discussion above Corollary 1.10, we see that $R_{\mathbb{Z}_p}(f)$ is maximal iff $a \equiv 0 \pmod{p^2}$. This is satisfied by $1/p$ of f in the above form; hence, $(p-1)/p$ proportion of forms in $T_p(1^21) \cup T_p(1^3)$ correspond to cubic rings maximal at p.

The two remarks above prove

Lemma 1.20.

$$\begin{aligned}\mu_p(\mathcal{U}_p(111)) =& \frac{1}{6}(p-1)^2p(p-1)/p^4\\ \mu_p(\mathcal{U}_p(12)) =& \frac{1}{2}(p-1)^2p(p+1)/p^4\\ \mu_p(\mathcal{U}_p(3)) =& \frac{1}{3}(p-1)^2p(p+1)/p^4\\ \mu_p(\mathcal{U}_p(1^21)) =& \ \ (p-1)^2\ \ (p+1)/p^4\\ \mu_p(\mathcal{U}_p(1^3)) =& \ \ (p-1)^2\ \ (p+1)/p^5\end{aligned}$$

For determining the average size of 3-torsion in quadratic class groups later on, we will need to consider the set $\mathcal{V}_p$ of elements $f \in \mathcal{U}_p$ such that $(f,p) \neq (1^3)$; this set parameterizes maximal cubic rings $R = R(f)$ which are maximal at p and not totally ramified at p.

From the above lemma, we obtain

Corollary 1.21 (of Lemma 1.20)**.**

$$\begin{aligned}\mu_p(\mathcal{U}_p) &= (p^3-1)(p^2-1)/p^5\\ \mu_p(\mathcal{V}_p) &= (p^2-1)^2/p^4\end{aligned}$$

2 Counting Cubic Rings

In this section, we obtain are first asymptotic results. Recall that $V_{\mathbb{R}}$ denotes the 4-dimensional vector space of binary cubic forms over $\mathbb{R}$. Let $V_{\mathbb{R}}^+, V_{\mathbb{R}}^- \subset V_{\mathbb{R}}$ denote the subsets consisting those forms with positive or negative, respectively, discriminant. These are the two orbits of the natural action of $\mathrm{GL}_2(\mathbb{R}) \curvearrowright (V_{\mathbb{R}} \setminus \{0\})$. We wish to understand the number

$$N\left(V_{\mathbb{Z}}^{\pm}; X\right)$$

of *irreducible* $\mathrm{GL}_2(\mathbb{Z})$-orbits on $V_{\mathbb{Z}}^{\pm} = V_{\mathbb{Z}} \cap V_{\mathbb{R}}^{\pm}$ having absolute discriminant less than X. Here, a $\mathrm{GL}_2(\mathbb{Z})$-orbit on $V_{\mathbb{Z}}$ si called **irreducible** if any (all) of its elements are irreducible over $\mathbb{Q}$.

The goal of this section is to prove

Theorem 2.1.

$$\begin{aligned}N\left(V_{\mathbb{Z}}^{+}; X\right) &= \frac{\pi^2}{72}X + o(X); \qquad \textit{and}\\ N\left(V_{\mathbb{Z}}^{-}; X\right) &= \frac{\pi^2}{24}X + o(X).\end{aligned}$$

Remark 2.2. [BST13] actually shows that the $o(X)$'s above can be replaced with $O(X^{5/6})$'s. We will be a little less careful and obtain instead $O(X^{11/12})$; we only care about the main term in these notes, so we find this acceptable.

Very roughly, since $\mathrm{GL}_2(\mathbb{R})$ acts transitively on $V_{\mathbb{R}}^{+}$, we will obtain Theorem 2.1 by counting lattice points in the space formed by the translates of some $v_{\pm} \in V_{\mathbb{Z}}^{\pm}$ under a fundamental domain for $\mathrm{GL}_2(\mathbb{Z})$ acting on $\mathrm{GL}_2(\mathbb{R})$; that is, we will morally be counting lattice points in $\mathrm{GL}_2(\mathbb{Z})\backslash\mathrm{GL}_2(\mathbb{R}) \cdot v_{\pm} \subset V_{\mathbb{R}}^{\pm} \cong \mathbb{R}^4$.

Notation 2.3. Because we are interested in proving a linear asymptotic, we will super careful in keeping track of lower order terms. To this end, we introduce the non-standard notation

$$f(x) \asymp g(x) \iff f(x) = g(x) + o(x).$$

We could just use $\sim$ instead of $\asymp$, except we will note know that $N(V_{\mathbb{Z}}^{\pm}; X)$ is asympotically linear in X until the end.

2.1 The Setup

We start by describing the Iwasawa decomposition for $\mathrm{GL}_2(\mathbb{R})$.

Notation 2.4. Let K, K_1, A_+, N, Λ denote the following subgroups of $\mathrm{GL}_2(\mathbb{R})$:

$$\begin{array}{ccccc}
K_1 & = & \{\text{orthogonal transformations in } \mathrm{GL}_2(\mathbb{R})\} & = & O_2(\mathbb{R}) \\
K & = & \left\{\begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} : \theta \in \mathbb{R}/2\pi i\mathbb{Z}\right\} & = & \mathrm{SO}_2(\mathbb{R}) \\
A_+ & = & \left\{ a_t := \begin{pmatrix} t^{-1} & \\ & t \end{pmatrix} : t \in \mathbb{R}_+ \right\} & \cong & \mathbb{R}_{>0}^{\times} \\
N & = & \left\{ n_u := \begin{pmatrix} 1 & \\ u & 1 \end{pmatrix} : u \in \mathbb{R} \right\} & \cong & \mathbb{R} \\
\Lambda & = & \left\{ \begin{pmatrix} \lambda & \\ & \lambda \end{pmatrix} : \lambda > 0 \right\} & \cong & \mathbb{R}_{>0}^{\times}
\end{array}$$

Proposition 2.5 (Iwasawa Decomposition). *The natural product*

$$\Lambda \times K_1 \times A_+ \times N \longrightarrow \mathrm{GL}_2(\mathbb{R})$$

is an analytic isomorphism.

Proof Sketch. We will only show that this map is surjective. We will see that, in constructing a preimage of a point, we really have a unique choice at each step so injectivity is at least plausible given the below argument.

Fix some $g \in \mathrm{GL}_2(\mathbb{R})$, and let $\lambda = |\det g|^{1/2}$. Let e_1, e_2 be the standard basis of $\mathbb{R}^2$, and define $v_i = g(e_i)$ $(i = 1, 2)$. Choose $k \in K_1$ such that $k(v_2)$ is a positive multiple of e_2. If $(kv_1, e_1) < 0$ then compose k with reflection across the e_2-axis, so we may assume that $(kv_1, e_1) \geq 0$. Write $kv_2 = se_2$ (so $s > 0$) and let $t = s^{-1} > 0$, so $a_t k(v_2) = e_2$. Write $a_t k(v_1) = \alpha e_1 + \beta e_2$ (so $\alpha > 0$). Then,

$$n_{-\beta/\alpha} a_t k(v_1) = n_{-\beta}(\alpha e_1 + \beta e_2) = \alpha e_1,$$

and $n_{-\beta/\alpha} a_t k(v_2) = e_2$. Let $T = n_{-\beta/\alpha} a_t k \lambda^{-1} g \in \mathrm{SL}_2(\mathbb{R})$. By construction $T(e_1) = \alpha e_1$ and $T(e_2) = e_2$, so $1 = \det T = \alpha$, which shows that $T = \mathrm{Id}$, i.e. that $g = \lambda k^{-1} a_{t^{-1}} n_{\beta/\alpha}$ is in the image of this map. ■

Remark 2.6. Fix $g \in \mathrm{GL}_2(\mathbb{R})$, and write $g^{-1} = \lambda kan$ with $\lambda \in \Lambda$, $k \in K_1$, $a \in A_+$, and $n \in N$. Then,

$g = n^{-1}a^{-1}k^{-1}\lambda^{-1}$, so one sees that the natural product

$$N \times A_+ \times K_1 \times \Lambda \longrightarrow \mathrm{GL}_2(\mathbb{R})$$

with the order of the factors reverse is also a bijection.

Notation 2.7. We will let $\mathcal{F} \subset \mathrm{GL}_2(\mathbb{R})$ denote Gauss's usual fundamental domain for $\mathrm{GL}_2(\mathbb{Z})\backslash\mathrm{GL}_2(\mathbb{R})$. This is

$$\mathcal{F} = \{nak\lambda : a \in A', n \in N'(a), k \in K, \lambda \in \Lambda\},$$

where

$$N'(a) = \left\{\begin{pmatrix} 1 & \\ n & 1\end{pmatrix} : n \in \nu(a)\right\}, \quad A' = \left\{\begin{pmatrix} t^{-1} & \\ & t\end{pmatrix} : t \geq \sqrt[4]{3}/\sqrt{2}\right\}, \quad \Lambda = \left\{\begin{pmatrix} \lambda & \\ & \lambda\end{pmatrix} : \lambda > 0\right\}.$$

Above, $\nu(a)$ is a union of either one or two subintervals of $[-1/2, 1/2]$ depending on the value of $a \in A'$. Specifically, if $a = a_t$, then $\nu(a)$ (which we may also call $\nu(t)$ from time to time) is

$$\nu(a_t) = \left\{n \in [-1/2, 1/2] : n^2 + t^4 = \left|n + t^2 i\right| \geq 1\right\}.$$

For verification that $\mathcal{F}$ is a fundamental domain for $\mathrm{GL}_2(\mathbb{Z}) \curvearrowright \mathrm{GL}_2(\mathbb{R})$, see [Lan20, Lemma 3.33].

To count irreducible binary cubics, it would suffice to be able to count lattice points in $\mathcal{F}v_\pm \subset V_\mathbb{R}^\pm$. The region $\mathcal{F}$ is not particularly nice-looking, so this is hard to do directly. In order to get around this instead of considering a single fundamental domain, we will count the average number of lattice points in $\mathcal{F}v$ as v ranges over a compact set $B \subset V_\mathbb{R}$. This has the advantage that the average number of lattice points in $\mathcal{F}v$ (for $v \in B$) is related to the average number of points in gB (for $g \in \mathcal{F}$) and we will be able to get a handle on this latter quantity using results from the geometry of numbers. With that said, let's get started.

Remark 2.8. Let $n_\pm$ denote the cardinality of the stabilizer in $\mathrm{GL}_2(\mathbb{R})$ of any (all) $v \in V_\mathbb{R}^\pm$. By Proposition 1.12, n_+ corresponds to the number of $\mathbb{R}$-algebra automorphisms of any cubic $\mathbb{R}$-algebra with positive discriminant, so $n_+ = \#\operatorname{Aut}_\mathbb{R}(\mathbb{R}^3) = 6$. Similarly, $n_- = \#\operatorname{Aut}(\mathbb{R} \oplus \mathbb{C}) = 2$. Now, note that, for $v \in V_\mathbb{R}^\pm$, $\mathcal{F}v$ will be the union of $n_\pm$ fundamental domains for the action of $\mathrm{GL}_2(\mathbb{Z})$ on $V_\mathbb{R}^\pm$. This union will not be disjoint, so *we view $\mathcal{F}v$ as a multiset* where each point $x \in \mathcal{F}v$ has multiplicity $\#\{g \in \mathcal{F} : gv = x\}$. That is, $x \in \mathcal{F}v$ has multiplicity $n_\pm/m(x)$, where $m(x) = \#\operatorname{Stab}_{\mathrm{GL}_2(\mathbb{Z})}(x)$. This is because $\{g \in \mathcal{F} : gv = x\}$ is in bijection with the group $\operatorname{Stab}_{\mathrm{GL}_2(\mathbb{R})}(x)/\operatorname{Stab}_{\mathrm{GL}_2(\mathbb{Z})}(x)$ via right-multiplication by any h satisfying $hx = v$.

Remark 2.9. From Proposition 1.12, we know that the stabilizer in $\mathrm{GL}_2(\mathbb{Z})$ of an irreducible element $x \in V_\mathbb{Z}$ is the group of ring automorphisms of the cubic ring $R = R(x)$ corresponding to x. This is equivalently the group of field automorphisms of the cubic number field $\operatorname{Frac} R(x)$, so we see that $\operatorname{Stab}_{\mathrm{GL}_2(\mathbb{Z})}(x)$ is either trivial of the cyclic group C_3 of order 3, when x is irreducible. Thus, for any $v \in V_\mathbb{R}^\pm$, the product $n_\pm \cdot N(V_\mathbb{Z}^\pm; X)$ is the number of irreducible integer points in $\mathcal{F}v$ having discriminant less than X, if we count C_3-orbits are counted with weight $1/3$ in $N(V_\mathbb{Z}^\pm; X)$.

That is, if we set

$$N(V_{\mathbb{Z}}^{\pm};X)=\sum_{\substack{x\in\mathrm{GL}_2(\mathbb{Z})\backslash V_{\mathbb{Z}}^{\pm}\\|\mathrm{Disc}\,x|<X}}\frac{1}{\#\,\mathrm{Stab}_{\mathrm{GL}_2(\mathbb{Z})}(x)}=\sum_{\substack{x\in\mathrm{GL}_2(\mathbb{Z})\backslash V_{\mathbb{Z}}^{\pm}\\|\mathrm{Disc}\,x|<X}}\frac{1}{\#\,\mathrm{Aut}_{\mathbb{Z}}(R(x))},$$

then $n_{\pm}N(V_{\mathbb{Z}}^{\pm};X)$ exactly counts the number of irreducible integer points in $\mathcal{F}v$ of absolute discriminant less than X ($v\in V_{\mathbb{Z}}^{\pm}$). We will see shortly that there are relatively few C_3-points – not enough for the difference in weighting to affect the main term in our asymptotics – so we will not stress this point too much.

Notation 2.10. Now that we have made the above remark, for any $\mathrm{GL}_2(\mathbb{Z})$-invariant set $S\subset V_{\mathbb{Z}}$, we set

$$N(S;X)=\sum_{\substack{x\in\mathrm{GL}_2(\mathbb{Z})\backslash S\\|\mathrm{Disc}\,x|<X}}\frac{1}{\#\,\mathrm{Stab}_{\mathrm{GL}_2(\mathbb{Z})}(x)}=\sum_{\substack{x\in\mathrm{GL}_2(\mathbb{Z})\backslash S\\|\mathrm{Disc}\,x|<X}}\frac{1}{\#\,\mathrm{Aut}_{\mathbb{Z}}(R(x))}.$$

As we mentioned this, directly counting these integral points would be difficult, so we will use an averaging trick to make the problem more tractable. Before doing this do, show that there are "few" reducible points, and "few" C_3-points so that, for the sake of proving $N(V_{\mathbb{Z}}^{\pm};X)\sim cX$ (for some $c\in\mathbb{R}$), we may ignore them.

Notation 2.11. Let $B\subset V_{\mathbb{R}}$ be come compact set. Given $v\in B$, we let

$$\mathcal{R}_X(v):=\{w\in\mathcal{F}v:|\mathrm{Disc}\,w|<X\}.$$

We first show that $\mathcal{R}_X(v)$ has few reducible elements. Note that if $f(x,y)=ax^3+bx^2y+cxy^2+dy^3$ has $a=0$, then it is reducible since it has y as a factor. Thus, in counting irreducible points, we can restrict to points with $a\neq 0$. With this in mind, we really show that $\mathcal{R}_X(v)$ has few irreducible points with $a\neq 0$.

Lemma 2.12. *Let $v\in B$ be any point of nonzero discriminant, where B is any fixed compact subset of $V_{\mathbb{R}}$ containing only elements having discriminant greater than 1. Then the number of integral binary cubic forms $ax^2+bx^2y+cxy^2+dy^3\in\mathcal{R}_X(v)$ that are reducible with $a\neq 0$ is $O(X^{3/4+\varepsilon})$, where the implied constant depends only on B.*

Proof. For an element $f(x,y)=ax^3+bx^2y+cxy^2+dy^3\in\mathcal{R}_X(v)$, we have $f\in N'A'K\Lambda v$ where $0<\lambda<X^{1/4}$, since $\mathrm{Disc}(\lambda\cdot v)=\lambda^4\,\mathrm{Disc}(v)$. This says that (recall $t\geq\sqrt[4]{3}/\sqrt{2}$, so t^{-1} bounded above)

$$\begin{aligned}f(x,y)&=\frac{1}{\det\gamma}v((x,y)\cdot\gamma)\\&=\frac{1}{\lambda^2}\cdot v\left((x,y)\cdot\begin{pmatrix}1&0\\n&1\end{pmatrix}\begin{pmatrix}t^{-1}&0\\0&t\end{pmatrix}\begin{pmatrix}\cos\theta&\sin\theta\\-\sin\theta&\cos\theta\end{pmatrix}\begin{pmatrix}\lambda&0\\0&\lambda\end{pmatrix}\right)\\&=\frac{\lambda^3}{\lambda^2}\cdot v\left((x,y)\cdot\begin{pmatrix}t^{-1}&0\\nt^{-1}&t\end{pmatrix}\begin{pmatrix}\cos\theta&\sin\theta\\-\sin\theta&\cos\theta\end{pmatrix}\right)\\&=\lambda\cdot v\left((x,y)\cdot\begin{pmatrix}t^{-1}\cos\theta&t^{-1}\sin\theta\\nt^{-1}\cos\theta-t\sin\theta&nt^{-1}\sin\theta+t\cos\theta\end{pmatrix}\right)\end{aligned}$$

$$= \lambda \cdot v\left(xt^{-1}\cos\theta + y(nt^{-1}\cos\theta - t\sin\theta), xt^{-1}\sin\theta + y(nt^{-1}\sin\theta + t\cos\theta)\right)$$

By considering the x^3 coefficient in the expansion of the last line above, we see that $a = O(\lambda t^{-3}) = O(X^{1/4})$. Similar considerations show that[3]

$$\begin{aligned}
a &= O(\lambda t^{-3}) &&= O(X^{1/4})\\
ab &= O(\lambda^2(t^{-4}+t^{-6})) &&= O(X^{2/4})\\
ac &= O(\lambda^2(t^{-2}+t^{-4}+t^{-6})) &&= O(X^{2/4})\\
ad &= O(\lambda^2(1+t^{-2}+t^{-4}+t^{-6})) &&= O(X^{2/4})\\
abc &= O(\lambda^3(t^{-3}+t^{-5}+t^{-7}+t^{-9})) &&= O(X^{3/4})\\
abd &= O(\lambda^3(t^{-1}+t^{-3}+t^{-5}+t^{-7}+t^{-9})) &&= O(X^{3/4})
\end{aligned}$$

From this we see that the total number of forms $f \in \mathcal{R}_X(v)$ with $a \neq 0$ and $d = 0$ is $O(X^{3/4+\varepsilon})$. This is essentially because there are $O(X^{1/4})$ choices for a, and hence $O(X^{1/4})$ choices for each of b, c as well since $ab, ac = O(X^{2/4})$.

Now assume $a \neq 0$ and $d \neq 0$. Similar reasoning gives that the above estimates then show that the total number of possibilities for the triple (a, b, d) is $O(X^{3/4+\varepsilon})$. Now suppose a, b, d are fixed ($d \neq 0$), and consider the number of possibilities for c so that $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$ is reducible. This requires it to have a linear factor $rx + sy$ with $r, s \in \mathbb{Z}$ coprime. Hence, r must be a factor of a, while s must be a factor of d. The number of divisors $\sigma_0(n)$ of a number n is $o(n^\varepsilon)$, so there are $o(X^\varepsilon)$ choices for the pair (r, s). Given a, b, d, r, s, one can recover c by solving $f(-s, r) = 0$, so we end up with $O(X^{3/4+\varepsilon})o(X^\varepsilon) = O(X^{3/4+\varepsilon})$ possibilities in this case as well. This finishes the proof. ■

We next show that there are few C_3-points in $\mathcal{R}_X(v)$, when v has positive discriminant. If v has negative discriminant, then there are no C_3-points in $\mathcal{R}_X(v)$. This is because, for $v \in V_{\mathbb{Z}}^-$, the cubic field $\operatorname{Frac} R(v)$ has a complex place; hence, writing $\operatorname{Frac} R(v) = \mathbb{Q}[x]/(g(x))$, two roots of g are complex conjugate pairs. Thus, 2 (the order of complex conjugation) divides the degree of the splitting fields of g, and so $\operatorname{Frac} R(v) \neq \operatorname{split}_{\mathbb{Q}} g(x)$.

Lemma 2.13. *Let $v \in V_{\mathbb{R}}$ be any point of positive discriminant. Then the number of integral points in $V_{\mathbb{Z}} \cap \mathcal{R}_X(v)$ having stabilizer C_3 in $\mathrm{GL}_2(\mathbb{Z})$ is $O(X^{3/4+\varepsilon})$, where the implied constant is independent of v.*

Proof. The number of integral points in $\mathcal{R}_X(v)$ having stabilizer C_3 in $\mathrm{GL}_2(\mathbb{Z})$ is equal to the number of isomorphism classes of cubic rings having automorphism group C_3 and discriminant less than X. This number is thus independent of v, so it suffices to prove the lemma for any single v with positive discriminant.

Let $v \in V_{\mathbb{Z}}$ be the binary cubic $x^3 - 3xy^2$. Every binary cubic form $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$ has an associated binary quadratic form, the **Hessian covariant**

$$H_f(x, y) := (b^2 - 3ac)x^2 + (bc - 9ad)xy + (c^2 - 3bd)y^2.$$

[3] All that really matters below is the exponent on λ and the fact that t never has a positive exponent

One can check by hand that, for $g \in \mathrm{SL}_2(\mathbb{R})$, one has $H_{g \cdot f}(x,y) = (g \cdot H_f)(x,y)$. For our choice of v, we have

$$H_v(x,y) = 9(x^2+y^2).$$

Fix some $g \in \mathcal{F} \cap \mathrm{SL}_2(\mathbb{R})$, and write

$$g = \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix} \begin{pmatrix} t^{-1} & 0 \\ 0 & t \end{pmatrix} \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}.$$

Then,

$$\begin{aligned}(g \cdot H_v)(x,y) &= H_v\left(xt^{-1}\cos\theta + y(nt^{-1}\cos\theta - t\sin\theta), xt^{-1}\sin\theta + y(nt^{-1}\sin\theta + t\cos\theta)\right) \\ &= 9\big[\left(t^{-2}\cos^2\theta + t^{-2}\sin^2\theta\right)x^2 + \\ &\qquad \left(nt^{-2}\cos^2\theta - \cos\theta\sin\theta + nt^{-2}\sin^2\theta + \sin\theta\cos\theta\right)xy + \\ &\qquad \left(n^2t^{-2}\cos^2\theta - 2n\cos\theta\sin\theta + t^2\sin^2\theta + n^2t^{-2}\sin^2\theta + 2n\sin\theta\cos\theta + t^2\cos^2\theta\right)y^2\big] \\ &= 9\left[t^{-2}x^2 + 2nt^{-2}xy + (n^2t^{-2}+t^2)y^2\right] \\ &= \frac{9\left[x^2 + 2nxy + (n^2+t^4)y^2\right]}{t^2}\end{aligned}$$

Recalling from Notation 2.7 that $|n| \leq 1/2$ and $n^2 + t^4 \geq 1$, we conclude that any quadratic form $A_1x^2 + A_2xy + A_3y^2$ in $\mathcal{F}H_v$ must satisfy $|A_2| \leq A_1 \leq A_3$. Thus, $\mathcal{F}v$ consists of binary cubic forms $f(x,y) = ax^3 + bx^2y + cxy^2 + dy^3$ satisfying

$$|bc - 9ad| \leq b^2 - 3ac \leq c^2 - 3bd.$$

Finally, if $f \in \mathcal{F}v$ has a nontrivial stabilizing element γ of order 3 in $\mathrm{SL}_2(\mathbb{Z})$, then γ will also stabilize H_f. However, the only reduced binary quadratic form, up to scaling, having a nontrivial order 3 stabilizing elements is $x^2 + xy + y^2$. Thus, any C_3-binary cubic $f(x,y) = ax^3 + bx^2y + cxy^2 + dy^3$ in $\mathcal{F}v$ will satisfy

$$|bc - 9ad| = b^2 - 3ac = c^2 - 3bd.$$

Hence, if a, b, d are fixed, then there are at most two solutions for c. Repeating the argument in Lemma 2.12, we see that the total number of possible triples (a,b,d) in $\mathcal{F}v$ is $O(X^{3/4+\varepsilon})$, so we win. ■

2.2 The Count

2.2.1 Averaging Trick

We can now carry out our averaging argument. We start with a simple lemma allowing us to interchange integrals over $\mathrm{GL}_2(\mathbb{R})$ with those over $V_{\mathbb{Z}}^{\pm}$.

Notation 2.14. Let $\mathcal{R}$ be a multiset, and let $\mathcal{R}_k$ denote its set of elements appearing with multiplicity exactly k. If $\mathcal{R}_k$ is measurable for all k, and $f : \mathcal{R} \to \mathbb{C}$ is a measurable function on $\mathcal{R}$'s underlying set, then we define

$$\int_{x \in \mathcal{R}} f(x)\mathrm{d}x := \sum_{k \geq 1} \int_{x \in \mathcal{R}_k} f(x)\mathrm{d}x.$$

Let $\mathrm{d}v$ denote the usual Euclidean measure on $V_{\mathbb{R}}$ (normalized so $V_{\mathbb{Z}}$ has co-volume 1), and let $\mathrm{d}g = t^{-2}\mathrm{d}n\mathrm{d}^{\times}t\mathrm{d}k\mathrm{d}^{\times}\lambda$ be the Haar measure of $\mathrm{GL}_2(\mathbb{R})$ obtained from its Iwasawa decomposition, with dk normalized to have measure 1 on $\mathrm{SO}_2(\mathbb{R})$. Then,

Proposition 2.15. *Let $f : V_{\mathbb{R}}^{\pm} \to \mathbb{C}$ be continuous, and choose any $v_{\pm} \in V_{\mathbb{R}}^{\pm}$. Then,*

$$\int_{g\in \mathrm{GL}_2(\mathbb{R})} f(g\cdot v_{\pm})\mathrm{d}g = \frac{1}{2\pi}\int_{v\in \mathrm{GL}_2(\mathbb{R})\cdot v_{\pm}} f(v)\left|\mathrm{Disc}(v)\right|^{-1}\mathrm{d}v = \frac{n_{\pm}}{2\pi}\int_{v\in V_{\mathbb{R}}^{\pm}} f(v)\left|\mathrm{Disc}\, v\right|^{-1}\mathrm{d}v.$$

Proof Sketch. For the first equality, one can explicitly compute the Jacobian for the change of variable sending $g \in \mathrm{GL}_2(\mathbb{R})$ to $v = g\cdot v_{\pm} \in V_{\mathbb{R}}$. The coordinates on g are the (k, t, n, λ) coming from the Iwasawa decomposition, while the coordinates on v are the usual (a, b, c, d) describing its corresponding form. To obtain the second equality, one simply uses that the multiset $\mathrm{GL}_2(\mathbb{R})\cdot v_{\pm}$ is an $n_{\pm}$-fold cover of $V_{\mathbb{R}}^{\pm}$. ■

In particular, we see that $\left|\mathrm{Disc}\, v\right|^{-1}\mathrm{d}v$ is a $\mathrm{GL}_2(\mathbb{R})$-invariant measure on $V_{\mathbb{R}}$ since, for $h \in \mathrm{GL}_2(\mathbb{R})$, we have (using that $\mathrm{d}g$ is a Haar measure)

$$\int_{v\in V_{\mathbb{R}}^{\pm}} f(h\cdot v)\left|\mathrm{Disc}\, v\right|^{-1}\mathrm{d}v = \frac{2\pi}{n_{\pm}}\int_{g\in \mathrm{GL}_2(\mathbb{R})} f(g\cdot h\cdot v_{\pm})\mathrm{d}g = \frac{2\pi}{n_{\pm}}\int_{g\in \mathrm{GL}_2(\mathbb{R})} f(g\cdot v_{\pm})\mathrm{d}g = \int_{v\in V_{\mathbb{R}}^{\pm}} f(v)\left|\mathrm{Disc}\, v\right|^{-1}\mathrm{d}v.$$

We proved a couple results at the end of the previous section which made use of an auxillary compact set $B \subset V_{\mathbb{R}}$. We know fix a choice of said set. Fix some $C \geq 1$, and let

$$B = B(C) := \left\{w = (a, b, c, d) \in V_{\mathbb{R}} : 3a^2 + b^2 + c^2 + 3d^2 \leq C \text{ and } \left|\mathrm{Disc}(w)\right| \geq 1\right\}.$$

Remark 2.16. B is $K = \mathrm{SO}_2(\mathbb{R})$-invariant. This is because a lengthy computation shows that the expression $3a^2 + b^2 + c^2 + 3d^2$ is itself invariant under the $\mathrm{SO}_2(\mathbb{R})$-action.

Let $V_{\mathbb{Z}}^{\mathrm{irr}}$ denote the subset of irreducible points of $V_{\mathbb{Z}}$. Recall from Remark 2.9 that

$$n_i N(V_{\mathbb{Z}}^{\pm}; X) = \#\left\{x \in \mathcal{F}v \cap V_{\mathbb{Z}}^{\mathrm{irr}} : \left|\mathrm{Disc}\, x\right| < X\right\},$$

and note that this equality in fact holds for any $\mathrm{GL}_2(\mathbb{Z})$-invariant subset $S \subset V_{\mathbb{Z}}^{\pm}$ taking the place of $V_{\mathbb{Z}}^{\pm}$. Since the number of integral points in $\mathcal{F}v \cap S^{\mathrm{irr}}$ is independent on the choice of $v \in S$, we obtain

$$N\left(S; X\right) = \frac{\int_{v\in B\cap V_{\mathbb{R}}^{\pm}} n_i N(S;X)\left|\mathrm{Disc}\, v\right|^{-1}\mathrm{d}v}{n_i\int_{v\in B\cap V_{\mathbb{R}}^{\pm}}\left|\mathrm{Disc}\, v\right|^{-1}\mathrm{d}v} = \frac{\int_{v\in B\cap V_{\mathbb{R}}^{\pm}}\#\left\{x \in \mathcal{F}v\cap S^{\mathrm{irr}} : \left|\mathrm{Disc}\, x\right| < X\right\}\left|\mathrm{Disc}\, v\right|^{-1}\mathrm{d}v}{n_i\int_{v\in B\cap V_{\mathbb{R}}^{\pm}}\left|\mathrm{Disc}\, v\right|^{-1}\mathrm{d}v} \tag{2.1}$$

We shall take (2.1) as the definition of $N(S; X)$ for $S \subset V_{\mathbb{Z}}$ not necessarily $\mathrm{GL}_2(\mathbb{Z})$-invariant. Note that for disjoint $S_1, S_2 \subset V_{\mathbb{Z}}$, one has $N(S_1 \sqcup S_2; X) = N(S_1; X) + N(S_2; X)$.

We would like to simplify the expression for $N(S, X)$ as much as possible. In particular, given that we have access to Proposition 2.15, we would like to be able to switch the roles of $\mathcal{F}$ and B, so that we may compute $N(S; X)$ by integrating over $\mathcal{F}$ (or a region in $\mathrm{GL}_2(\mathbb{R})$ like it), and counting lattice points in B (or a compact in $V_{\mathbb{R}}$ like it) instead.

Fix $v_{\pm} \in V_{\mathbb{R}}^{\pm}$, and choose maximal subsets $H^{\pm} \subset \mathrm{GL}_2(\mathbb{R})$ such that $H^{\pm}\cdot v_{\pm} = B \cap V_{\mathbb{R}}^{\pm}$. So, the multiset $H^{\pm} \cdot v_{\pm}$ is an $n_{\pm}$-fold cover of $B \cap V_{\mathbb{R}}^{\pm}$. The numerator on the RHS of (2.1) is now equal to

$$\begin{aligned}\int_{v \in B \cap V_{\mathbb{R}}^{\pm}} \#\left\{x \in \mathcal{F}v \cap S^{\mathrm{irr}} : |\mathrm{Disc}\, x| < X\right\} |\mathrm{Disc}\, v|^{-1} \mathrm{d}v &= \sum_{x \in S^{\mathrm{irr}} : |\mathrm{Disc}\, x| < X} \int_{v \in B \cap V_{\mathbb{R}}^{\pm}} \#\left\{g \in \mathcal{F} : x = gv\right\} |\mathrm{Disc}\, v|^{-1} \mathrm{d}v \\ &= \frac{2\pi}{n_{\pm}} \sum_{x \in S^{\mathrm{irr}} : |\mathrm{Disc}\, x| < X} \int_{h \in H^{\pm}} \#\{g \in \mathcal{F} : x = ghv_{\pm}\} \mathrm{d}h \\ &= \frac{2\pi}{n_{\pm}} \sum_{\substack{x \in S^{\mathrm{irr}} \\ |\mathrm{Disc}\, x| < X}} \int_{g \in \mathcal{F}} \#\left\{h \in H^{\pm} : x = ghv_{\pm}\right\} \mathrm{d}g \\ &= \frac{2\pi}{n_{\pm}} \int_{g \in \mathcal{F}} \#\left\{x \in S^{\mathrm{irr}} \cap gH^{\pm}v_{\pm} : |\mathrm{Disc}\, x| < X\right\} \mathrm{d}g. \end{aligned} \tag{2.2}$$

The second equality comes from Proposition 2.15. Note that we have succeeded in interchanging the roles of $\mathcal{F}$ and $B \cap V_{\mathbb{R}}^{\pm} = H^{\pm}v_{\pm}$. We can still rewrite things slightly. Recall that $KB = B$ and that $\int K \mathrm{d}k = 1$. Any $g \in \mathcal{F}$ can be written in the form $g = hk$ with $h \in N'(a)A'\Lambda$ and $k \in K$, so (2.2) is further equal to

$$\begin{aligned}&\frac{2\pi}{n_{\pm}} \int\limits_{h \in N'(a)A'\Lambda} \int\limits_{k \in K} \#\left\{x \in S^{\mathrm{irr}} \cap hkB \cap V_{\mathbb{R}}^{\pm} : |\mathrm{Disc}\, x| < X\right\} \mathrm{d}h\mathrm{d}k \\ =&\frac{2\pi}{n_{\pm}} \int\limits_{h \in N'(a)A'\Lambda} \int\limits_{k \in K} \#\left\{x \in S^{\mathrm{irr}} \cap hB \cap V_{\mathbb{R}}^{\pm} : |\mathrm{Disc}\, x| < X\right\} \mathrm{d}h\mathrm{d}k \\ =&\frac{2\pi}{n_{\pm}} \left(\int\limits_{h \in N'(a)A'\Lambda} \#\left\{x \in S^{\mathrm{irr}} \cap hB \cap V_{\mathbb{R}}^{\pm} : |\mathrm{Disc}\, x| < X\right\} \mathrm{d}h \right) \left(\int\limits_{k \in K} \mathrm{d}k \right) \\ =&\frac{2\pi}{n_{\pm}} \int\limits_{h = na_t\lambda \in N'(a)A'\Lambda} \#\left\{x \in S^{\mathrm{irr}} \cap na_t\lambda B \cap V_{\mathbb{R}}^{\pm} : |\mathrm{Disc}\, x| < X\right\} \mathrm{d}h,\end{aligned}$$

where $\mathrm{d}h = t^{-2}\mathrm{d}n\mathrm{d}^{\times}t\mathrm{d}^{\times}\lambda$. Let

$$B(n, t, \lambda, X) = n \begin{pmatrix} t^{-1} & \\ & t \end{pmatrix} \lambda B \cap \left\{v \in V_{\mathbb{R}}^{\pm} : |\mathrm{Disc}\, v| < X\right\}.$$

We have shown that

$$N(S; X) = \frac{1}{M_{\pm}} \int_{g \in N'(a)A'\Lambda} \#\left\{x \in S^{\mathrm{irr}} \cap B(n, t, \lambda, X)\right\} t^{-2}\mathrm{d}n\mathrm{d}^{\times}t\mathrm{d}^{\times}\lambda \tag{2.3}$$

where

$$M_{\pm} := M_{\pm}(C) = \frac{n_{\pm}}{2\pi} \int_{v \in B(C) \cap V_{\mathbb{R}}^{(i)}} |\mathrm{Disc}\, v|^{-1} \mathrm{d}v.$$

2.2.2 Estimating Lattice Points

By equation (2.3), in order to get good asymptotics for $N(V_{\mathbb{Z}}^{\pm}; X)$, we will want good estimates for the number of lattice points in $B(n, t, \lambda, X)$. To do so, we will use version of theorem of Davenport which is applicable to multisets.

Definition 2.17. A multiset $\mathcal{R} \subset \mathbb{R}^n$ is called **mesurable** if $\mathcal{R}_k$ is measurable for all k, where $\mathcal{R}_k$ denotes the set of those points in $\mathcal{R}$ having multiplicity exactly k. Given a measurable multiset $\mathcal{R} \subset \mathbb{R}^n$, we define its **volume** to be

$$\mathrm{Vol}(\mathcal{R}) = \sum_k k \cdot \mathrm{Vol}(\mathcal{R}_k),$$

where $\mathrm{Vol}(\mathcal{R}_k)$ denotes the usual Euclidean volume of $\mathcal{R}_k$.

Theorem 2.18 (See [Dav51] and [Dav64])**.** *Let $\mathcal{R}$ be a bounded multiset in $\mathbb{R}^n$ having maximum multiplicity m, and which is defined by at most k polynomial inequalities each having degree at most ℓ. Let $\mathcal{R}'$ denote the image of $\mathcal{R}$ under any (upper or lower) triangular, unipotent transformation of $\mathbb{R}^n$. Then the number of integer lattice points (counted with multiplicity) contained in the region $\mathcal{R}'$ is*

$$\mathrm{Vol}(\mathcal{R}) + O(\max\{\mathrm{Vol}(\overline{\mathcal{R}}), 1\})$$

where $\mathrm{Vol}(\overline{\mathcal{R}})$ denote the greatest d-dimensional volume of any projection of $\mathcal{R}$ onto a coordinate subspace obtained by equating $n-d$ coordinates to zero, where d takes all values from 1 to $n-1$. The implied constant in the second summands depends only on n, m, k, and ℓ.

Corollary 2.19. *The number of lattice points (a, b, c, d) in $B(n, t, \lambda, X) \subset V_{\mathbb{R}}^{\pm}$ with $a \neq 0$ is*

$$\begin{cases} 0 & \text{if } C\lambda < t^3 \\ \mathrm{Vol}(B(n,t,\lambda,X)) + O(\max\{C^3\lambda^3 t^4, 1\}) & \text{otherwise} \end{cases}$$

Proof. First note than any binary cubic in $B(n, t, \lambda, X)$ is of the form $na_t\lambda v$ for some cubic $v = (a', b', c', d') \in B$ (in particular, $a' \leq C$), i.e. is of the form

$$(na_t\lambda v)(x, y) = \frac{1}{\lambda^2} v\left((x, y) \cdot \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix} \begin{pmatrix} t^{-1} & 0 \\ 0 & t \end{pmatrix} \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}\right) = \lambda v\left(t^{-1}x + t^{-1}ny, ty\right),$$

and so has x^3 coefficient $a'\lambda/t^3 \leq C\lambda/t^3$. This gives the first case in the claim; if $C\lambda/t^3 < 1$, then any $(a, b, c, d) \in B(n, t, \lambda, X)$ must have $a = 0$.

If $C\lambda/t^3 \geq 1$, then λ and t are positive numbers bounded from below by $(\sqrt[4]{3}/\sqrt{2})^3/C$ and $\sqrt[4]{3}/\sqrt{2}$, respectively. One can easily check that for any $(a, b, c, d) \in B(n, t, \lambda, X)$, one has

$$\begin{aligned} a &= O(C\lambda t^{-3}) &&= O(C\lambda t^{-3}) \\ b &= O(C\lambda(t^{-1} + t^{-3})) &&= O(C\lambda t^{-1}) \\ c &= O(C\lambda(t + t^{-1} + t^{-3})) &&= O(C\lambda t) \\ d &= O(C\lambda(t^3 + t + t^{-1} + t^{-3})) &&= O(C\lambda t^3) \end{aligned}$$

Maximizing the exponents of each factor individually, it is clear that each coordinate projection of $B(n, t, \lambda, X)$ has volume at most $O(C^3\lambda^3 t^4)$. ■

Remark 2.20. [BST13] obtain a $O(\max\{C^3\lambda^3 t^3, 1\})$ where t has exponent 3 instead of 4. Recalling Remark 2.2, this is the reason they obtain a smaller $o(X)$ term in Theorem 2.1 than we do.

In the above corollary, we only consider the points with $a \neq 0$ since we ultimately only want to count irreducible integral points in $B(n, t, \lambda, X)$.

Recall 2.21 (Notation 2.3)**.** We have adopted the notation

$$f(x) \asymp g(x) \iff f(x) = g(x) + o(x).$$

In (2.3), the integrand will be nonzero only if $t^3 \leq C\lambda$ (by Corollary 2.19) and $\lambda \leq X^{1/4}$ (since B consists only of points having discriminant at least 1). Thus, we may write, up to an error of $O(X^{3/4+\varepsilon})$ (due to Lemma 2.12), that

$$N(V_{\mathbb{Z}}^{\pm}; X) \asymp \frac{1}{M_{\pm}} \int_{\lambda=(\sqrt[4]{3}/\sqrt{2})^3/C}^{X^{1/4}} \int_{t=\sqrt[4]{3}/\sqrt{2}}^{C^{1/3}\lambda^{1/3}} \int_{N'(t)} \left(\mathrm{Vol}(B(n, t, \lambda, X)) + O(\max\{C^3\lambda^3 t^4, 1\})\right) t^{-2} \mathrm{d}n \mathrm{d}^{\times}t \mathrm{d}^{\times}\lambda. \tag{2.4}$$

The integral of the first summand in (2.4) is (note the limits for t)

$$\frac{1}{2\pi M_{\pm}} \int_{v \in B \cap V_{\mathbb{R}}^{\pm}} \mathrm{Vol}(\mathcal{R}_X(v)) \left|\mathrm{Disc}\, v\right|^{-1} \mathrm{d}v - \frac{1}{M_{\pm}} \int_{\lambda=(\sqrt[4]{3}/\sqrt{2})^3/C}^{X^{1/4}} \int_{t=C^{1/3}\lambda^{1/3}}^{\infty} \int_{N'(t)} \mathrm{Vol}(B(n, t, \lambda, X)) t^{-2} \mathrm{d}n \mathrm{d}^{\times}t \mathrm{d}^{\times}\lambda. \tag{2.5}$$

Now, as a consequence of Proposition 2.15, $\mathrm{Vol}(\mathcal{R}_X(v))$ does not depend on the choice of $v \in V_{\mathbb{R}}^{\pm}$. Since $\mathrm{Vol}(B(n, t, \lambda, X)) = O(C^4\lambda^4)$, e.g. from the estimates on the coordinates of any $w \in B(n, t, \lambda, X)$ given in the proof of Corollary 2.19, we see that (2.5) is equal to

$$\frac{\mathrm{Vol}(\mathcal{R}_X(v))}{n_{\pm}} + O\left(\frac{C^{10/3}X^{5/6}}{M_{\pm}(C)}\right).$$

What about the second summand in (2.4)? This is

$$\begin{aligned} \frac{1}{M_{\pm}} \int_{\lambda=(\sqrt[4]{3}/\sqrt{2})^3/C}^{X^{1/4}} \int_{t=\sqrt[4]{3}/\sqrt{2}}^{C^{1/3}\lambda^{1/3}} \int_{N'(t)} O(\max\{C^3\lambda^3 t^4, 1\}) t^{-2} \mathrm{d}n \mathrm{d}^{\times}t \mathrm{d}^{\times}\lambda &= \int_{\lambda=(\sqrt[4]{3}/\sqrt{2})^3/C}^{X^{1/4}} \int_{t=\sqrt[4]{3}/\sqrt{2}}^{C^{1/3}\lambda^{1/3}} O\left(\frac{C^3\lambda^3 t^2}{M_{\pm}(C)}\right) \mathrm{d}^{\times}t \mathrm{d}^{\times}\lambda \\ &= \int_{\lambda=(\sqrt[4]{3}/\sqrt{2})^3/C}^{X^{1/4}} O\left(\frac{C^{11/3}\lambda^{11/3}}{M_{\pm}(C)}\right) \mathrm{d}^{\times}\lambda \\ &= O\left(\frac{C^{11/3}X^{11/12}}{M_{\pm}(C)}\right) \end{aligned}$$

All these remains at this point in computing $\mathrm{Vol}(\mathcal{R}_X(v_{\pm}))$ for any fixed $v_{\pm} \in V_{\mathbb{R}}^{\pm}$. Proposition 2.15 tells us that the measure $2\pi \left|\mathrm{Disc}\, v_{\pm}\right| \lambda^4 \mathrm{d}g/n_{\pm}$ pushes forward, along the map $g \mapsto g \cdot v_{\pm}$, to the usual measure Euclidean measure $\mathrm{d}v$ on $V_{\mathbb{R}}^{\pm} \cong \mathbb{R}^4$. We may assume $\left|\mathrm{Disc}\, v_{\pm}\right| = 1$. Lemma 2.13 tells us that, up to $O(X^{3/4+\varepsilon}) = o(X)$ error, every point in the multiset $\mathcal{R}_X(v_{\pm})$ has multiplicity $n_{\pm}$, so

$$\frac{\mathrm{Vol}(\mathcal{R}_X(v))}{n_{\pm}} \asymp \frac{2\pi}{n_{\pm}} \int_{\lambda=0}^{X^{1/4}} \lambda^4 \mathrm{d}^{\times}\lambda \int_{h \in N'(a)A'K} \mathrm{d}h = \frac{2\pi}{n_{\pm}} \frac{X^4}{4} \frac{\pi}{6} = \frac{\pi^2}{12 n_{\pm}} X,$$

where we have quoted [BST13, Beginning of Section 5.4] in using that

$$\int_{h \in N'(a)A'K} \mathrm{d}h = \mathrm{Vol}(\mathrm{GL}_2(\mathbb{Z}) \backslash \mathrm{GL}_2^{\pm}(\mathbb{R})) = \frac{\pi}{6}.$$

Combining the various displayed equations in this section, we have shown

$$\begin{aligned}
N(V_{\mathbb{Z}}^{\pm};X) &\asymp \frac{1}{M_{\pm}}\int_{\lambda=(\sqrt[4]{3}/\sqrt{2})^3/C}^{X^{1/4}}\int_{t=\sqrt[4]{3}/\sqrt{2}}^{C^{1/3}\lambda^{1/3}}\int_{N'(t)}\big(\mathrm{Vol}(B(n,t,\lambda,X))+O(\max\{C^3\lambda^3t^4,1\})\big)\,t^{-2}\mathrm{d}n\mathrm{d}^{\times}t\mathrm{d}^{\times}\lambda\\
&=\left[\frac{\mathrm{Vol}(\mathcal{R}_X(v))}{n_{\pm}}+O\left(\frac{C^{10/3}X^{5/6}}{M_{\pm}(C)}\right)\right]+O\left(\frac{C^{11/3}X^{11/12}}{M_{\pm}(C)}\right)\\
&=\frac{\pi^2}{12n_{\pm}}X+O(X^{11/12})
\end{aligned}$$

which proves Theorem 2.1.

2.3 Including Congruence Conditions

Now that we have Theorem 2.1, we would like to use results from Section 1.2 to obtain an asymptotic count of maximal irreducible cubic rings from our current count of irreducible cubic rings. This will involving placing infinitely many local maximality conditions on our rings, one for each prime p. As a stepping stone to a result allowing us to do this, we first obtain a version of Theorem 2.1 which allows for a finite number of local conditions.

Theorem 2.22. *Fix an integer $m \geq 1$, and consider the natural projection maps $q_{\pm} : V_{\mathbb{Z}}^{\pm} \subset V_{\mathbb{Z}} \cong \mathbb{Z}^4 \twoheadrightarrow (\mathbb{Z}/m\mathbb{Z})^4$. Let $S = q_{\pm}^{-1}(\overline{S}) \subset V_{\mathbb{Z}}^{\pm}$ for some $\overline{S} \subset (\mathbb{Z}/m\mathbb{Z})^4$; we say that S is **defined by finitely many congruence conditions**. Then,*

$$\lim_{X\to\infty}\frac{N(S\cap V_{\mathbb{Z}}^{\pm};X)}{X}=\frac{\pi^2}{12n_{\pm}}\prod_{p\mid m}\mu_p(S),$$

i.e. $N(S\cap V_{\mathbb{Z}}^{\pm};X) = \left(\frac{\pi^2}{12n_i}\prod_p \mu_p(S)\right)X + o(X)$, where $\mu_p(S)$ denotes the p-adic density of S in $V_{\mathbb{Z}}$, $n_+ = 6$, and $n_- = 2$.

To obtain Theorem 2.22, suppose that $S \subset V_{\mathbb{Z}}^{\pm}$ is defined by finitely congruence conditions, so $S = q_{\pm}^{-1}(\overline{S})$ for some $\overline{S} \subset (\mathbb{Z}/m\mathbb{Z})^4$. Then, $S = V_{\mathbb{Z}}^{\pm} \cap U$ where U is the union of $k = \#\overline{S}$ translates $L_1, \dots, L_k$ of the lattice $m \cdot V_{\mathbb{Z}}$. If $\overline{S} = \{q_{\pm}(e_1), \dots, q_{\pm}(e_k)\}$ with $e_1, \dots, e_k \in V_{\mathbb{Z}}^{\pm}$, then $L_i = m \cdot V_{\mathbb{Z}} + e_i$. For each lattice translate L_j, we use formula (2.3) along with the discussion following it to compute $N(L_j \cap V_{\mathbb{Z}}^{(i)}; X)$, where each d-dimensional volume is scaled by a factor of $1/m^d$ to reflect the fact that our new lattice has been scaled by a factor of m. With these scalings, the volumes of the $d = 3, 2, 1$ dimensional projections of $B(n, t, \lambda, X)$ are seen to be at most $O\left(m^{-3}C^3t^3\lambda^3\right)$, $O\left(m^{-2}C^2t^4\lambda^2\right)$, $O\left(m^{-1}Ct^3\lambda\right)$, respectively, so they are all at most $O(m^{-3}C^3t^4\lambda^3)$.[4] Let $a \geq 1$ be the smallest nonzero first coordinate of any point in L_j. Then, analogous to Corollary 2.19, the number of lattice points in $B(n, t, \lambda, X) \cap L_j$ with first coordinate nonzero is

$$\begin{cases} 0 & \text{if } C\lambda t^{-3} < a \\ \frac{\mathrm{Vol}(B(n,t,\lambda,X))}{m^4} + O\left(\frac{C^3t^4\lambda^3}{m^3}\right) & \text{otherwise} \end{cases}$$

Carrying out the integral for $N(L_j; X)$ as before, we obtain, up to $O(X^{3/4+\varepsilon})$ error (coming from Lemma

[4] Not combining these three bounds yet would get one an $O(X^{5/6})$ error in the end, instead of a $O(X^{11/12})$ error

2.12) that

$$N(L_j \cap V_{\mathbb{Z}}^{(i)}; X) \asymp \frac{\mathrm{Vol}(\mathcal{R}_X(v))}{m^4 n_\pm} + O\left(\frac{C^{10/3} X^{11/12}}{M_\pm(C) a^{1/3} m^3}\right).$$

Summing over the k values of j, this gives

$$N(S; X) \asymp \frac{k}{m^4} \frac{\mathrm{Vol}(\mathcal{R}_X(v))}{n_\pm} + O\left(\frac{k X^{11/12}}{m^3}\right).$$

Finally, Theorem 2.22 follow from

$$\frac{k}{m^4} = \prod_p \mu_p(S) \text{ and } \frac{\mathrm{Vol}(\mathcal{R}_X(v))}{n_\pm} \asymp \frac{\pi^2}{12 n_\pm} X.$$

3 Wrapping Things Up

We are in the home stretch now. All that remains is to obtain a version of Theorem 2.22 allowing for infinitely many congruence conditions, and apply it using the densities for $\mathcal{U}_p$ obtained in Corollary 1.21. In order to carry this out, we will need a uniform estimate on the error terms appearing when only finitely many conditions are taken into account, so we obtain this first.

As before, let $\mathcal{V}_p$ denote the set of all $f \in V_{\mathbb{Z}}$ for which $R(f)$ is maximal at p, but in which p does not totally ramify. Furthermore, let $\mathcal{Z}_p = V_{\mathbb{Z}} - \mathcal{V}_p$. We can and do partition this as $\mathcal{Z}_p = \mathcal{W}_p \sqcup \mathcal{Y}_p$ where $\mathcal{W}_p$ consists of all forms $f \in V_{\mathbb{Z}}$ whose corresponding cubic rings are *not* maximal at p, while $\mathcal{Y}_p$ consist of all forms whose ring *is* maximal at p, but *is* also totally ramified there.

3.1 Counting Cubic Number Fields

Lemma 3.1. *Let $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$ be an integral binary cubic form, and let $g = \gcd(a, b, c, d)$. Then, g is the maximal integer n such that $R(f) = \mathbb{Z} + nR'$ for some other cubic ring R'. We call this value g the* ***content*** *of f (or of $R(f)$), and denote it by either of $\mathrm{ct}(f) = \mathrm{ct}(R(f))$.*

Proof Sketch. This is a consequence of (1.3). ■

Proposition 3.2. *$N(\mathcal{W}_p; X) = O(X/p^2)$, where the implied constant is independent of p.*

Proof. Let us say that a cubic ring R is **primitive at** p if $p \nmid \mathrm{ct}(R)$. From Proposition 1.11, we easily see that if R is primitive at p, then it has at most 3 index p subrings. At present, we wish to bound the number of cubic rings which are not maximal at p, and which have absolute discriminant less than X. Suppose R is such a ring. By Lemma 1.9, it has a $\mathbb{Z}$-basis $\langle 1, \omega, \theta \rangle$ such that one of

$$\begin{array}{lll} \textbf{(i)} & R' = \mathbb{Z} + \mathbb{Z}(\omega/p) + \mathbb{Z}\theta & \left[\mathrm{Disc}(R') = \mathrm{Disc}(R)/p^2\right] \\ \textbf{(ii)} & R'' = \mathbb{Z} + \mathbb{Z}(\omega/p) + \mathbb{Z}(\theta/p) & \left[\mathrm{Disc}(R'') = \mathrm{Disc}(R)/p^4\right] \end{array}$$

is also a cubic ring.

Assume first that we are in base **(i)**. Then, $\mathrm{Disc}(R') < X/p^2$, so there are at most $O(X/p^2)$ possible choices for R', by Theorem 2.1. If R' is primitive at p, then since R is index p in R', there are at most 3 possible R for each R', so this gives $O(X/p^2)$ choices for R when R' primitive at p. If R' is not primitive at

p, there exists a ring S such that $R' = \mathbb{Z} + pS$. Note that $R' \subset S$ is index p^2 since $S/R' = (S/\mathbb{Z})/p(S/\mathbb{Z})$, so $R \subset S$ is index p^3 and $\mathrm{Disc}(S) = \mathrm{Disc}(R)/p^6 < X/p^6$. Hence, again by Theorem 2.1, there are $O(X/p^6)$ choices for S, and so the same number of choices for $R' = \mathbb{Z}+pS$. Finally, since $\mathbb{Z}^2 \cong (R/\mathbb{Z}) \subset (R'/\mathbb{Z}) \cong \mathbb{Z}^2$ is index p, there can at most post $p+1$ choice of R given R', so we get $O((p+1)X/p^6)$ choices for R when R' is not primitive at p. All in all, there are $O(X/p^2) = O(X/p^2) + O((p+1)X/p^6)$ choices for R in case **(i)**.

Now, assume we are in case **(ii)**. Then, $R = \mathbb{Z}+pR''$ and $\mathrm{Disc}(R'') < X/p^4$. Hence, there are $O(X/p^4)$ choices for R'', and so the same number of choices for R. Thus, $N(\mathcal{W}_p; X) = O(X/p^2) + O(X/p^4) = O(X/p^2)$ as claimed. ■

The above proposition suffices to get the asymptotic count of cubic fields. For determining the average size of 3-torsion in class groups, however, we will also need an analogous result for $N(\mathcal{Y}_p; X)$, i.e. we will need to bound the number of cubic fields not ramified at p. We will obtain this later. For now, let's prove Theorem 1.

Let $\mathcal{U} = \bigcap_p \mathcal{U}_p$. Then, $\mathcal{U}$ is the set of $v \in V_{\mathbb{Z}}$ corresponding to maximal cubic rings R. Recall that Corollary 1.21 shows us that the p-adic density of $\mathcal{U}_p$ is $\mu_p(\mathcal{U}_p) = (1-p^{-2})(1-p^{-3})$. Suppose Y is any positive integer. Theorem 2.22 let's us see that

$$\lim_{X\to\infty} \frac{N\left(\bigcap_{p<Y} \mathcal{U}_p \cap V_{\mathbb{Z}}^{\pm}; X\right)}{X} = \frac{\pi^2}{12 n_{\pm}} \prod_{p<Y} \left(1-p^{-2}\right)\left(1-p^{-3}\right).$$

We would like to prove (the second equality in)

$$\begin{aligned}
\lim_{X\to\infty} \frac{N\left(\mathcal{U} \cap V_{\mathbb{Z}}^{\pm}; X\right)}{X} &= \lim_{X\to\infty}\lim_{Y\to\infty} \frac{N\left(\bigcap_{p<Y} \mathcal{U}_p \cap V_{\mathbb{Z}}^{\pm}; X\right)}{X} \\
&= \lim_{Y\to\infty}\lim_{X\to\infty} \frac{N\left(\bigcap_{p<Y} \mathcal{U}_p \cap V_{\mathbb{Z}}^{\pm}; X\right)}{X} \\
&= \lim_{Y\to\infty} \frac{\pi^2}{12 n_{\pm}} \prod_{p<Y} \left(1-p^{-2}\right)\left(1-p^{-3}\right) \\
&= \frac{\pi^2}{12 n_{\pm}} \frac{1}{\zeta(2)\zeta(3)} \\
&= \frac{1}{2 n_{\pm} \zeta(3)}. \qquad (3.1)
\end{aligned}$$

This would give Theorem 1. For notational convenience, set

$$N_Y(X) := \frac{N\left(\bigcap_{p<Y} \mathcal{U}_p \cap V_{\mathbb{Z}}^{\pm}; X\right)}{X} \text{ and } N(X) := \frac{N\left(\mathcal{U} \cap V_{\mathbb{Z}}^{\pm}; X\right)}{X}.$$

To switch the limits in (3.1), it will suffice to show that

$$\lim_{Y\to\infty}\lim_{X\to\infty} \frac{N_Y(X) - N(X)}{X} = 0.$$

Using Proposition 3.2, this holds because

$$\frac{N_Y(X) - N(X)}{X} = \frac{N\left(\bigcup_{p\geq Y} \mathcal{W}_p \cap V_{\mathbb{Z}}^{\pm}; X\right)}{X} \leq \frac{O(X)\sum_{p\geq Y} p^{-2}}{X} = O(1)\sum_{p\geq Y} p^{-2} \xrightarrow{Y\to\infty} 0$$

with the tail vanishing in the limit since the sum $\sum_p p^{-2} \leq \zeta(2)$ is convergent. Finally, taking $\lim\limits_{Y\to\infty}\lim\limits_{X\to\infty}$ of

$$\frac{N(X)}{X} = \frac{N_Y(X)}{X} - \frac{N_Y(X) - N(X)}{X}$$

now gives

$$\lim_{X\to\infty} \frac{N\left(\mathcal{U} \cap V_{\mathbb{Z}}^{\pm}; X\right)}{X} = \lim_{X\to\infty}\frac{N(X)}{X} = \lim_{Y\to\infty}\lim_{X\to\infty}\frac{N_Y(X)}{X} = \frac{1}{2n_{\pm}\zeta(3)}$$

as desired.

3.2 Average Size of 3-torsion in Class Groups of Quadratic Number Fields

We begin by explaining the connection between cubic fields and 3-torsion in the class groups of quadratic fields.

Let $F/\mathbb{Q}$ be a quadratic field, and let H_F denote its Hilbert class field, so H_F/F is F's maximal abelian, unramified extension, and $\mathrm{Gal}(H_F/F) \simeq \mathrm{Cl}_F$. Since $\mathrm{Cl}_F[3] = \mathrm{Hom}(\mathrm{Cl}_F, C_3) = \mathrm{Hom}(\mathrm{Gal}(H_F/F), C_3)$, we see that each nontrivial element of $\mathrm{Cl}_F[3]$ gives an unramified C_3-extension L/F of F (including an iso $\mathrm{Gal}(L/F) \xrightarrow{\sim} C_3$). Since $\#\,\mathrm{Aut}(C_3) = 2$, we see that every unramified C_3-extension L/F has two isomorphisms $\mathrm{Gal}(L/F) \xrightarrow{\sim} C_3$, and so corresponds to 2 nontrivial elements of $\mathrm{Cl}_F[3]$. Thus, the number of unramified C_3-extensions of F is $\frac{\#\,\mathrm{Cl}_F[3]-1}{2}$.

Fact. Let $K/\mathbb{Q}$ be a non-Galois cubic field. Let $L/\mathbb{Q}$ be the Galois closure of K, so $\mathrm{Gal}(L/\mathbb{Q}) \simeq S_3$, and L has a unique quadratic subfield $F/\mathbb{Q}$. This situation is summed up in the diagram

$$\begin{tikzcd}
& L \arrow[dl, dash, "2"'] \arrow[dr, dash, "C_3"] & \\
K \arrow[dr, dash, "3"'] & & F \arrow[dl, dash, "2"] \\
& \mathbb{Q} &
\end{tikzcd}$$

In this situation, $\mathrm{Disc}(K) = f^2\,\mathrm{Disc}(F)$ where f is the conductor of L/F, equal to the product of rational primes totally ramifying in $K/\mathbb{Q}$.

The above fact tells us that counting C_3-extensions of F is roughly the same thing as counting non-Galois cubics (which, by Lemma 2.13 is 'almost all cubics'). Recall that we had earlier defined the set $\mathcal{Y}_p$, consisting of cubic fields not totally ramified at p, and let $\mathcal{V} = \bigcap_p \mathcal{V}_p$. We see now that

$$\sum_{0<\mathrm{Disc}(F)<X} \frac{\#\,\mathrm{Cl}_F[3]-1}{2} \asymp N(\mathcal{V}\cap V_{\mathbb{Z}}^{+}; X)$$

$$\sum_{-X<\mathrm{Disc}(F)<0} \frac{\#\,\mathrm{Cl}_F[3]-1}{2} \asymp N(\mathcal{V}\cap V_{\mathbb{Z}}^{-}; X), \tag{3.2}$$

where the $\asymp$ again denotes up to $o(X)$ (coming from the cyclic cubics). This is the connection we will exploit. To perform another sieve in order the count unramified cubics (hence the average size of $\mathrm{Cl}_F[3]$), we will need a good bound for $N(\mathcal{Y}_p; X)$. We obtain this below.

Notation 3.3. Given a number field F, let $C_F = \mathbb{A}_F^\times / F^\times$ denote its idèle class group, so C_3-extensions of F correspond to continuous surjections $C_F \twoheadrightarrow C_3$.

For $f \in \mathbb{Z}_{\geq 1}$, let $\omega(f)$ denote its number of rational prime divisors.

Lemma 3.4. *The number of closed, index* 3 *subgroups* $H \subset C_F$ *is* $O\left(9^{\omega(f)} \# \mathrm{Cl}_F[3]\right)$.

Proof. The group C_F fits into an exact sequence[5]

$$1 \longrightarrow \frac{\prod_v \mathscr{O}_v^\times}{\mathscr{O}_F^\times} \longrightarrow C_F \longrightarrow \mathrm{Cl}_F \longrightarrow 1,$$

where the product is taken over places v of F. Taking $\mathrm{Hom}(-, C_3)$, we obtain the exact sequence

$$0 \longrightarrow \mathrm{Hom}(\mathrm{Cl}_F, C_3) \longrightarrow \mathrm{Hom}(C_F, C_3) \longrightarrow \mathrm{Hom}\left(\frac{\prod_v \mathscr{O}_v^\times}{\mathscr{O}_F^\times}, C_3\right). \tag{3.3}$$

Now, note that the notion of the conductor of a map $C_F \to C_3$ equally makes sense for a map $\frac{\prod_v \mathscr{O}_v^\times}{\mathscr{O}_F^\times} \to C_3$, and the restriction map $\mathrm{Hom}(C_F, C_3) \longrightarrow \mathrm{Hom}\left(\frac{\prod_v \mathscr{O}_v^\times}{\mathscr{O}_F^\times}, C_3\right)$ above preserves conductors. With this in mind, we will introduce an ^{f} superscript to indicate the subset of maps of conductor f, e.g. $\mathrm{Hom}(C_F, C_3)^f$. The sequence (3.3) tells us that

$$\left|\mathrm{Hom}\left(C_F, C_3\right)^f\right| \leq |\mathrm{Hom}(\mathrm{Cl}_F, C_3)| \left|\mathrm{Hom}\left(\frac{\prod_v \mathscr{O}_v^\times}{\mathscr{O}_F^\times}, C_3\right)^f\right| \leq |\mathrm{Hom}(\mathrm{Cl}_F, C_3)| \left|\mathrm{Hom}\left(\prod_v \mathscr{O}_v^\times, C_3\right)^f\right|. \tag{3.4}$$

Now, each $p \mid f$ has at most 2 places v above it in F, so the number of places of F at which L/F ramifies is at most $2\omega(f)$. For such such place, $\# \mathrm{Hom}(\mathscr{O}_v^\times, C_3) \leq 3$ if $v \nmid 3$. There are only finitely many $v \mid 3$, and for each such v, $\mathbb{Q}_v$ is a quadratic extension of $\mathbb{Q}_3$; since there only only finitely many such extensions, $\# \mathrm{Hom}(\mathscr{O}_v^\times, C_3)$ is uniformly bounded for $v \mid 3$. This combined with (3.4) gives

$$\# \mathrm{Hom}(C_F, C_3)^f = O\left(3^{2\omega(f)} \# \mathrm{Cl}_F[3]\right)$$

as claimed. ■

Proposition 3.5. $N(\mathcal{Y}_p; X) = O(X/p^2)$, *where the implied constant is independent of* p.

Proof. Recall that the discriminant of a non-cyclic cubic field K is of the form $\mathrm{Disc}(K) = f^2 \mathrm{Disc}(F)$ where F is the unique quadratic subfield of the Galois closure of $K/\mathbb{Q}$. Combining this with Lemmas 2.13 and 3.4, we see that

$$N(\mathcal{Y}_p; X) = O\left(\sum_{f>0, p \mid f} \sum_{\substack{F \text{ quad} \\ \pm \mathrm{Disc}(f) \leq X/f^2}} 9^{\omega(f)} \# \mathrm{Cl}_F[3]\right) + O(X^{3/4+\varepsilon}).$$

[5] If $v \mid \infty$, we set $\mathscr{O}_v^\times = F_v$

We expect the first summand to be linear in X, so we ignore the second summand for now. Note that

$$\sum_{\substack{F \text{ quad} \\ \pm \operatorname{Disc}(F) \le X/f^2}} \# \operatorname{Cl}_F[3] = N(\mathcal{V} \cap V_{\mathbb{Z}}^{\pm}; X/f^2) + o(X) \le N(V_{\mathbb{Z}}^{\pm}; X/f^2) + o(X) = O(X/f^2).$$

Hence (using $p \mid f \iff f = mp$),[6]

$$N(\mathcal{Y}_p; X) \asymp O\left(\sum_{m \ge 1} 9^{\omega(m)} \sum_{\substack{F \text{ quad} \\ \pm \operatorname{Disc}(f) \le X/(mp)^2}} \# \operatorname{Cl}_F[3] \right) = O\left(\sum_m 9^{\omega(m)} \frac{X}{p^2 m^2} \right) = O\left(\frac{X}{p^2} \sum_{m \ge 1} \frac{9^{\omega(m)}}{m^2} \right) = O\left(\frac{X}{p^2} \right),$$

where we have used that

$$\sum_{m \ge 1} \frac{9^{\omega(m)}}{m^2} = \prod_{\ell} \left(1 + \frac{9}{\ell^2} + \frac{9}{\ell^4} + \cdots \right) \le \prod_{\ell} \left(1 - \frac{9}{\ell^2} \right)^{-1} < \infty \text{ since } \sum_{\ell} \frac{9}{\ell^2} < \infty.$$

This finishes the proof. ■

Corollary 3.6. *$N(\mathcal{Z}_p; X) = O(X/p^2)$, where the implied constant is independent of p.*

Proof. Recalling that $\mathcal{Z}_p = \mathcal{W}_p \cup \mathcal{Y}_p$, this is Propositions 3.2 and 3.5. ■

This brings us to the end. The proof of Theorem 1 in section 3.1 (the part after Proposition 3.2) works equally well in the present case (with $\mathcal{U}_p$ replaced by $\mathcal{V}_p$, $\mathcal{W}_p$ replaced by $\mathcal{Z}_p$, and Proposition 3.2 replaced by Corollary 3.6) to show that

$$\lim_{X \to \infty} \frac{N(\mathcal{V} \cap V_{\mathbb{Z}}^{\pm}; X)}{X} = \frac{\pi^2}{12 n_{\pm}} \prod_p (1 - p^{-2})^2 = \frac{\pi^2}{12 n_{\pm}} \frac{1}{\zeta(2)^2} = \frac{3}{n_{\pm} \pi^2}.$$

Using (3.2) along with the well-known fact[7]

$$\lim_{X \to \infty} \frac{\sum_{0 < \operatorname{Disc}(K_2) < X} 1}{X} = \frac{3}{\pi^2} = \lim_{X \to \infty} \frac{\sum_{-X < \operatorname{Disc}(K_2) < 0} 1}{X},$$

we now obtain

$$\lim_{X \to \infty} \frac{\sum_{0 < \operatorname{Disc}(K_2) < X} h_3^*(K_2)}{\sum_{0 < \operatorname{Disc}(K_2) < X} 1} = 1 + 2 \lim_{X \to \infty} \frac{N(\mathcal{V} \cap V_{\mathbb{Z}}^{+}; X)}{\sum_{0 < \operatorname{Disc}(K_2) < X} 1} = 1 + 2 \frac{3/(6\pi^2)}{3/\pi^2} = 1 + \frac{6}{18} = \frac{4}{3}$$

and

$$\lim_{X \to \infty} \frac{\sum_{-X < \operatorname{Disc}(K_2) < 0} h_3^*(K_2)}{\sum_{-X < \operatorname{Disc}(K_2) < 0} 1} = 1 + 2 \lim_{X \to \infty} \frac{N(\mathcal{V} \cap V_{\mathbb{Z}}^{-}; X)}{\sum_{-X < \operatorname{Disc}(K_2) < 0} 1} = 1 + 2 \frac{3/(2\pi^2)}{3/\pi^2} = 1 + \frac{6}{6} = 2.$$

This is Theorem 2.

[6] Below, we have $\omega(m)$ instead of $\omega(mp)$ since $\omega(mp) \le \omega(m) + 1$, and this 1 only contributes a factor of 9 to the expression

[7] Every quadratic field F is of the form $F = \mathbb{Q}(\sqrt{\operatorname{Disc} F})$, so this basically amounts to counting square-free integers

Recalling the basic observation $\#\operatorname{Sur}(\mathrm{Cl}_F, \mathbb{Z}/3\mathbb{Z}) = \#\,\mathrm{Cl}_F[3] - 1$ all the way from the introduction – along with the motivation coming from Cohen-Lenstra's predicted statistics for class groups of quadratic fields and the notation $\mu_X^\pm$ – this in turn gives

$$\lim_{X\to\infty} \mathbb{E}_{F\sim\mu_X^+}\left[\#\operatorname{Sur}\left(\mathrm{Cl}_F, \frac{\mathbb{Z}}{3\mathbb{Z}}\right)\right] = \lim_{X\to\infty} \mathbb{E}_{F\sim\mu_X^+}[\#\,\mathrm{Cl}_F[3]-1] = \frac{4}{3} - 1 = \frac{1}{3}$$
$$\lim_{X\to\infty} \mathbb{E}_{F\sim\mu_X^-}\left[\#\operatorname{Sur}\left(\mathrm{Cl}_F, \frac{\mathbb{Z}}{3\mathbb{Z}}\right)\right] = \lim_{X\to\infty} \mathbb{E}_{F\sim\mu_X^-}[\#\,\mathrm{Cl}_F[3]-1] = 2 - 1\ = 1$$

as desired.

References

[BST13] Manjul Bhargava, Arul Shankar, and Jacob Tsimerman. On the Davenport-Heilbronn theorems and second order terms. *Invent. Math.*, 193(2):439–499, 2013.

[CL84] H. Cohen and H. W. Lenstra, Jr. Heuristics on class groups of number fields. In *Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983)*, volume 1068 of *Lecture Notes in Math.*, pages 33–62. Springer, Berlin, 1984.

[Dav51] H. Davenport. On a principle of Lipschitz. *J. London Math. Soc.*, 26:179–183, 1951.

[Dav64] H. Davenport. Corrigendum: "On a principle of Lipschitz". *J. London Math. Soc.*, 39:580, 1964.

[DH71] H. Davenport and H. Heilbronn. On the density of discriminants of cubic fields. II. *Proc. Roy. Soc. London Ser. A*, 322(1551):405–420, 1971.

[GGS02] Wee Teck Gan, Benedict Gross, and Gordan Savin. Fourier coefficients of modular forms on G_2. *Duke Math. J.*, 115(1):105–169, 2002.

[Lan20] A. Landesman. Notes on counting extensions of degrees 2 and 3, following bhargava. https://web.stanford.edu/ aaronlan/assets/bhargavology-seminar-notes.pdf, 2020.